Amendments to the Claims

Please cancel Claims 7 and 20. Please amend Claims 1-5, 8-18, 21, and 22. Please add new Claims 23 and 24. The Claim Listing below will replace all prior versions of the claims in the application:

Claim Listing

1. (Currently amended) A system for ~~journaling activity~~ providing a usage accountability model for data security in a data processing system comprising:

   a user client device having a sensor to sense atomic level events at a point of authorized access to at least one digital asset by an end user of the user client device, the sensor located within an operating system kernel within [[a]] the user client device; and

   a journaling server having an aggregator to accept ~~multiple~~ the atomic level events from the user client device and to aggregate at least some of the atomic level events to generate [[an]] at least one aggregate event based on [[a]] at least one predetermined sequence of atomic level events, and having a reporter to generate an audit trail from the at least one aggregate event, the audit trail representing usage of the at least one digital asset by the end user.

2. (Currently amended) A system as [[is]] in claim 1 wherein the aggregate events are associated with a particular executing process.

3. (Currently amended) A system as [[is]] in claim 2 wherein the executing process is associated with ~~a particular~~ the end user.

4. (Currently amended) A system as in claim 1 ~~additionally comprising:~~ wherein the user client device further includes a filter for filtering the atomic level events with an approved event list, and wherein the aggregator only accepts atomic level events not filtered out by the filter.

5. (Currently amended) A system as [[is]] in claim 4 wherein the approved event list includes a list of approved file identifiers.

6. (Previously presented) A system as in claim 5 wherein the file identifiers are a hash code.

7. (Canceled)

8. (Currently amended) A system as in ~~claim 7 additionally comprising:~~ claim 1 wherein the user client device further includes a coalescer to coalesce ~~multiple~~ at least some of the atomic events output by the sensor into a single event prior to inputting them to the aggregator.

9. (Currently amended) A system as in claim 8 wherein a bundle of coalesced events is created prior to their transmission between the ~~agent~~ user client device and the journaling server.

10. (Currently amended) A system as in claim 9 wherein sequence numbers are added to the bundles.

11. (Currently amended) A system as in claim 1 wherein [[an]] the at least one aggregate event is detected as a suspect action with a data file.

12. (Currently amended) A system as in claim 1 wherein [[an]] the at least one aggregate event is attributable to ~~a known~~ the end user, a thread and/or an application as identified at a known time.

13. (Currently amended) A system as in claim 8 wherein the coalescer reports [[an]] a single coalesced event after a time out period with no activity.

14. (Currently amended) A system as in claim 1 wherein the at least one aggregate ~~events~~ event and the audit trail are used to control security of the data processing system by determining patterns of unexpected behavior based on the at least one aggregate event and the audit trail.

15. (Currently amended) A system as in claim 1 wherein the aggregate events ~~are used to~~ and the audit trail provide a perimeter of accountability for ~~file~~ usage of the at least one digital asset at a point of ~~system~~ use of the at least one digital asset.

16. (Currently amended) A system as in claim 15 wherein the point of use is [[a]] the user ~~desktop~~ client device and the accountability is of access, modification, and distribution of ~~data files~~ the at least one digital asset.

17. (Currently amended) A method for ~~journaling activity~~ providing a usage accountability model for data security in a data processing system comprising:

sensing atomic level events at a point of authorized access to at least one digital asset by an end user of a user client device of the data processing system, the sensing taking place in an operating system kernel within [[a]] the user client device; ~~and~~

forwarding the atomic level events to a journaling server of the data processing system;

aggregating ~~multiple~~ at least some of the atomic level events at the journaling server to generate [[an]] at least one aggregate event based on [[a]] at least one predetermined sequence of atomic level events; and

generating an audit trail from the at least one aggregate event, the audit trail representing usage of the at least one digital asset by the end user.

18. (Currently amended) A method as in claim 17 ~~additionally comprising:~~ further including filtering the atomic level events with an approved event list, and wherein forwarding the atomic level events to the journaling server includes forwarding only atomic level events not filtered out by the approved event list.

19. (Original) A method as in claim 18 where the approved event list includes a list of approved file identifiers.

20. (Canceled)

21. (Currently amended) A method as in ~~claim 20 additionally comprising:~~ claim 17 further including coalescing ~~multiple~~ at least some of the atomic events ~~output by the sensing step~~ into a single event prior to ~~providing them~~ forwarding the atomic level events to the ~~aggregating step~~ journaling server.

22. (Currently amended) A method as in claim 21 where a bundle of coalesced events is created prior to ~~a step of transmitting them between the client agent and~~ forwarding the atomic level events to the journaling server.

23. (New) A system as in claim 1 wherein the usage of the at least one digital asset includes access and dissemination of the at least one digital asset.

24. (New) A method as in claim 17 wherein the usage of the at least one digital asset includes access and dissemination of the at least one digital asset.